TL

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/963,789	09/27/2001	Keisuke Takemori	011152	9137

38834 7590 08/25/2005

WESTERMAN, HATTORI, DANIELS & ADRIAN, LLP
1250 CONNECTICUT AVENUE, NW
SUITE 700
WASHINGTON, DC 20036

EXAMINER	
PYZOCHA, MICHAEL J	
ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 08/25/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/963,789	**Applicant(s)** TAKEMORI ET AL.
	Examiner Michael Pyzocha	**Art Unit** 2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 July 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *2-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *2-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *22 July 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-20 are pending.

2. Amendment filed 07/22/2005 has been received and considered.

Drawings

3. The replacement drawings for figures 1-2, 5-8 were received on 07/22/2005. These drawings are accepted.

Claim Objections

4. The claim objections have been withdrawn based on the filed amendments.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 2-11, 14-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over ITL as applied to claim 1 above, and further in view of Golan (US 5974549).

As per claim 2, ITL discloses an intrusion preventing system which prevents an intrusion to regular data storage means connected to a network, comprising: decoy data storage means which is provided separately from the regular data storage means; and guiding means which guides an illegal access to the regular data storage means into the decoy data storage means (see page 4 column 3).

ITL fails to disclose the decoy and regular data storage means are on the same server, with the decoy means being secured.

However, Golan teaches such regions on the same system (see column 2 lines 13-28).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Golan's method of secure regions in the IDS system of ITL.

Motivation to do so would have been to only allow certain APIs to execute (see Golan column 2 lines 39-48).

As per claim 3, the modified ITL and Golan system discloses destination rewriting means, which rewrites a destination of an access, which is the server to the decoy region (see ITL page 4).

As per claim 4, the modified ITL and Golan system discloses response rewriting means which rewrites the content of a response command returned in response to an access to the decoy region to the content of a response command which is to be returned in response to an access to the regular region (see ITL page 4).

As per claims 5-7, the modified ITL and Golan system discloses monitors whether or not an access whose destination is the regular region is an illegal access, wherein the destination rewriting means rewrites the destination of an illegal access to the decoy region (see ITL page 4).

As per claim 8, the modified ITL and Golan system discloses the regular region and the decoy region are allocated with a common IP address (see ITL page 4 as applied to the cited Golan sections).

As per claim 9, the modified ITL and Golan system discloses means that collects action logs or trace data of a session guided to the decoy region (see ITL page 4).

As per claim 10, the modified ITL and Golan system discloses the regular data storage means is a regular server, and the decoy data storage means is a decoy server provided together with the regular server (see ITL page 4 column 3).

As per claim 11, the modified ITL and Golan system discloses intrusion judging means which judges whether or not a communication session established between the regular server and an external terminal is due to intrusion; communication session relaying means which relays a communication session which has been judged as an intrusion from the regular server to the decoy server; and path switching means which transfers a packet whose destination is the regular sever to the decoy server in a communication session which has been judged as the intrusion (see ITL page 4 column 3 and page 2 column 3 which discloses a packet-based IDS).

As per claims 14-15, the modified ITL and Golan system discloses a buffer for transfer which sequentially stores the same packets as packets whose destinations are the regular server; and a buffer for return which sequentially returns responses returned from the decoy server, wherein, when the communication session which has been judged as the intrusion is relayed to the decoy server, the buffer for transfer sequentially outputs the responses from the first packet which has been returned in response to the first packet transferred after relayed (see ITL page 4).

As per claim 16, the modified ITL and Golan system discloses pseudo response means which, without transferring a packet whose destination has been converted from the regular server to the decoy server, creates a response command to the packet in a pseudo manner to return the same (see ITL page 4).

As per claim 17, the modified ITL and Golan system discloses when a source address of a communication session, which has been judged as intrusion is stored and a packet containing the source address is then input, a communication session is established between the decoy server and the user (see ITL page 4).

As per claim 18, the modified ITL and Golan system discloses in the communication session established between the decoy server and the user, action logs and trace data of the user are collected (see ITL page 4).

As per claim 19, the modified ITL and Golan system discloses the path switching means includes means which converts the content of the response command returned from the decoy server to the content of a response command which will be output when the regular server receives a packet (see ITL page 4 where this is inherent because if this step did not occur the user would know it has be switched to a different server).

As per claim 20, the modified ITL and Golan system discloses an intrusion preventing system which prevents an intrusion to a regular region of a server connected to a network, wherein without allowing access to the regular region for an access command whose destination is the regular region, a pseudo response command expressing a message where the access to the regular region has been succeeded is returned response to the access to the regular region (see ITL page 4 column 3).

7. Claims 12-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified ITL and Golan system as applied to claim 10 above, and further in view of FOLDOC.

As per claims 12-13, the modified ITL and Golan system fails to disclose the response from the decoy server would be the same (or mirrored) as the regular server.

However, FOLDOC teaches mirroring (see page 1).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use mirroring from FOLDOC with the IDS of the modified ITL and Golan system.

Motivation to do so would have been to protect the data (see FOLDOC page 1).

Response to Arguments

8. Applicant's arguments filed 07/22/2005 have been fully considered but they are not persuasive. Applicant argues: ITL fails to disclose the regular data storage means is a regular server, and the decoy data storage means is a decoy server; ITL further fails to disclose system, and this claim specifies that, for an access attempt to the regular region, a pseudo response command is returned that expresses a message that the access to the regular region has succeeded; Golan fails to teach redirecting the downloaded software; and Golan does not disclose which parts of the system reside on the same server.

Regarding Applicant's argument that ITL fails to disclose the regular data storage means is a regular server, and the decoy data storage means is a decoy server, in the 3rd column of page 4 ITL discloses an IDS (which detects intrusions on a computer, the regular server, in a network), and when an attacker is detected, "the attacker is then seamlessly transferred to a special padded cell host." The padded cell host is the decoy server.

Regarding Applicant's argument that ITL fails to disclose system, and this claim specifies that, for an access attempt to the regular region, a pseudo response command is returned that expresses a message that the access to the regular region has succeeded, ITL as discussed above transfers an attacker to a padded cell host, once connected to the padded cell host it must appear to be the regular host or the attacker will immediately know. Therefore upon a request by the client (the attacker) a response (a message) would be returned as though it came from the regular server.

Regarding Applicant's argument that Golan fails to teach redirecting the downloaded software, Golan is only relied upon for the teaching of a secure memory area within one system and ITL is relied upon for the redirection.

Regarding Applicant's argument that Golan does not disclose which parts of the system reside on the same server as described in column 5 lines 37-59 of Golan the sandbox resides on a single system.

Applicant further requested a photocopy of page 4 with the relied upon subject matter clearly annotated. Examiner believes based on the above arguments it is clear what subject matter is relied upon.

Conclusion

9. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Shawcross (US 6880090) discloses the use of a decoy server.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Pyzocha whose telephone number is (571) 272-3875. The examiner can normally be reached on 7:00am - 4:30pm first Fridays of the bi-week off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJP

Matthew D Smithers
MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137